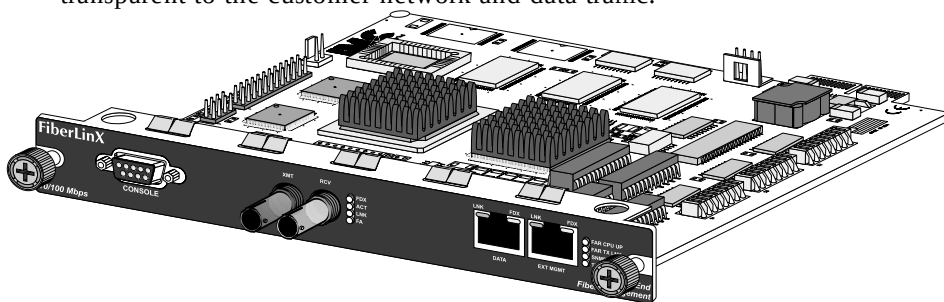


FiberLinX TX/FX™

Installation Guide

About FiberLinX TX/FX

FiberLinX TX/FX™ from IMC Networks is a SNMP-manageable networking device for provisioning point-to-point fiber optic connections between two locations. The primary advantage of *FiberLinX TX/FX* is End-to-End management, which allows the device administrator to monitor the fiber run between the head-end and remote site as a single entity, not as two separate locations. *FiberLinX* allows the device administrator to manage the remote unit without having access to the remote site, allowing the administrator to remain isolated and completely transparent to the customer network and data traffic.



A FiberLinX TX/FX Module

Installation Instructions

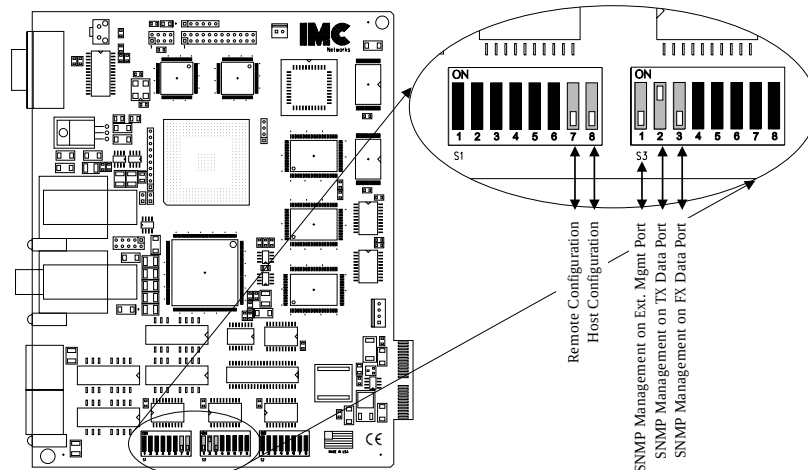
Installing a *FiberLinX TX/FX Module* involves the following steps: 1) configuring the *FiberLinX TX/FX Module* via its eight-position DIP switches for SNMP-Management and mode configuration, 2) designation of the management traffic port, 3) configuration of host/remote or standalone operation and auto-negotiation; along with the installation of the *FiberLinX TX/FX* module into a *PowerChassis/101* or */113* (not for use with *PowerChassis/1*, */2* or */12*).

► DIP SWITCH SETTINGS

Before installing *FiberLinX TX/FX* into a *PowerChassis*, you must configure the eight-position DIP switch, located at positions **S1** and **S3** (shown on the following page), for configuring the module.

QUICK START

Introduction	1
DIP Switch Settings	2
FiberAlert	3
Assigning IP Information	4
Using iView	8
If Not Using iView	9
Application Examples	10
LED Indicators	13
Tech Support	14



DIP Switch Location on FiberLinX TX/FX (default settings shown)

The following table shows the function for each of the eight DIP switches on *FiberLinX TX/FX*. Refer to the following pages for specific configuration information for each function.

SWITCH/POSITION	FUNCTION	DEFAULT
Switch S1		
1 - 6	Factory Configured — DO NOT CHANGE	Varies
7	Remote Configuration	OFF
8	Host Configuration	OFF
Switch S3		
1	SNMP Management Traffic for the TX Mgmt. Port	OFF
2	SNMP Management Traffic for the TX Data Port	ON
3	SNMP Management Traffic for the FX Data Port	OFF
4 - 8	Factory Configured — DO NOT CHANGE	Varies

► CONFIGURING FIBERLINX TX/FX AS A HOST, REMOTE OR STANDALONE UNIT

When two *FiberLinX TX/FX* units are paired with one another, each *FiberLinX TX/FX* unit can be configured to be either a **Host** unit or a **Remote** unit.

As a *Host*, *FiberLinX TX/FX* requests management information from any attached remote unit and displays that information, along with its own, upon SNMP query. As a *Remote*, *FiberLinX TX/FX* will not respond to requests for management information from an attached unit. In single installation, the sole *FiberLinX TX/FX* should be configured as standalone unit (factory default). The table on the following page shows the possible DIP switch settings. Please see page 10 of this guide for possible installations and their related *Host*, *Remote* and *standalone* DIP switch settings.

HOST AND REMOTE DIP SWITCHES (SWITCH S1)		
Switch 7	Switch 8	Result
OFF	OFF	Standalone Configuration (no Host or Remote) DEFAULT
ON	OFF	Remote Unit Configuration (Slave)
OFF	ON	Host Unit Configuration (Master)

Configure *FiberLinX TX/FX* to be a *Host* unit by setting DIP switch 8 on Switch **S1** to **ON**. Configure *FiberLinX TX/FX* to be a *Remote* unit by setting DIP switch 7 to **ON**. For a standalone module, set both DIP switches 7 and **8** to the OFF position.

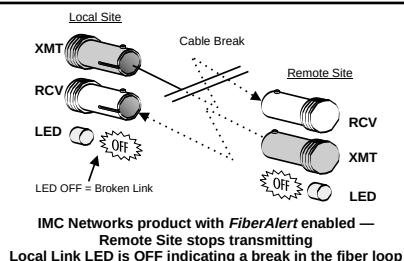
► SNMP MANAGEMENT TRAFFIC

Although *FiberLinX TX/FX* provides a twisted pair port solely for management traffic, you can configure *FiberLinX TX/FX* to accept SNMP management traffic from any of its three ports. There are four different ways you can configure *FiberLinX TX/FX* to accept (or not accept) SNMP management traffic. Only one source for SNMP management traffic can be active at any time, and only the SNMP management traffic directed to the module's IP address will be accepted.

FiberLinX TX/FX is configured at the factory to accept SNMP management traffic from the twisted pair *data* port, with DIP switch 2 on switch **S3 ON**, DIP switch 1 and **3 OFF**. You can change this setting by adjusting DIP switches **1** through **3**.

About FiberAlert

FiberAlert is an advanced troubleshooting feature that can help you locate "silent failures" on your network. However, it is vital that you understand exactly how *FiberAlert* works, and how it will react in your network configuration, before attempting to install the enclosed module.



Installing modules without understanding the effects of *FiberAlert* can cause perfectly functional units to appear flawed or even dead!

FiberAlert lets you know when a fault occurs on your fiber loop by stopping data transmissions and affecting the fiber LEDs on both sides of your network. Since *FiberLinX TX/FX* is a transparent link in a network, the *FiberAlert* feature, a troubleshooting feature that assists in pinpointing link faults between products, is implemented. If *FiberLinX TX/FX* is not receiving

a fiber link, *FiberAlert* disables its fiber transmitter, thus mirroring the link status of the opposite end of the fiber. Both fiber link LEDs on either side of the devices should extinguish, alerting you to the fault. Using *FiberAlert*, a local site administrator is notified of a fault and can quickly determine where a cable fault is located without having to go to the remote site.

NOTE

FiberAlert should only be activated on one side of a media extender. Activating the feature on both sides would keep both transmitters off indefinitely.

More information on *FiberAlert* can be found on the IMC Networks Web site at www.imcnetworks.com/to-fa.htm.

Installation Instructions

Once the DIP switches are set, you are ready to install *FiberLinX TX/FX*, which can be installed into any *PowerChassis/100* or */113* chassis.

To install *FiberLinX TX/FX*, remove the blank bracket covering the slot, if necessary, where you will be installing the module, then slide the module into the chassis, via the cardguides, until the module is seated securely in the connector. Secure the module to the chassis by tightening the captive screws. Once the module is installed, you will need to assign an IP address to the unit, which can be done via **HUBCTRL32™** (Hub Control 32) or serial configuration.

Assigning IP Information

In order for *FiberLinX TX/FX* to allow for SNMP-management, the module must be assigned IP configuration information (e.g., IP address, subnet mask, etc.). There are two ways to do this:

- Using **HUBCTRL32** over an Ethernet connection
- Using the unit's serial port

Besides assigning an IP address and subnet mask, the two methods will also allow you to create community strings, assign access rights, configure traps and more. However, **HUBCTRL32** offers more options than the serial port method (e.g., you can select *which* traps to assign with **HUBCTRL32**). Note that if you are using **HUBCTRL32**, you must have the SNMP/**HUBCTRL32** Function enabled via DIP switch (see Figure 2 on page 2 for details).

Once *FiberLinX TX/FX* is assigned an IP address, you can use *iView* or another SNMP-compatible Network Management System (NMS) to remotely configure, monitor and manage the media conversion modules installed in the unit (see page 8 of this guide for more information).

► ABOUT HUBCTRL32

HUBCTRL32 is an in-band configuration utility created by IMC Networks that lets users quickly and easily complete the first stages of SNMP configuration for IMC Networks SNMP-manageable devices.

Tasks *HUBCTRL32* can perform include:

- setting the IP address, subnet mask and default gateway
- defining the community strings and SNMP traps

In addition to the above functions, *HUBCTRL32* offers an authorized IP address system and access restriction to MIB groups supported by IMC Networks manageable devices. These extra layers of security are purely optional and do not affect SNMP compatibility in any way.

HUBCTRL32 can also be used to upload new versions of the system software and new MIB information. It also offers diagnostic capabilities for faster resolution of technical support issues.

HUBCTRL32 works with the following platforms:

- Windows 98™
- Windows NT™
- Windows 2000™

HUBCTRL32 can be found on the *iView* CD, or you can download it from the IMC Networks Web site (www.imcnetworks.com/tech/software). For information regarding the use of *HUBCTRL32*, refer to the *HUBCTRL32* online help file.

► ABOUT SERIAL PORT CONFIGURATION

FiberLinX TX/FX features a serial port that uses an IBM-compatible DB-9 serial connector. To connect *FiberLinX TX/FX* to your terminal/computer, use a straight-through (pin-to-pin) cable. (If your computer/terminal has a serial port using a connection not compatible with a DB-9 COM port, use the pin connection chart on the right for reference in making a cable.) Make sure the cable length is under 50 ft. (15.24 m). Plug one end of the cable into the DB-9 connector on *FiberLinX TX/FX* and the other into the appropriate port on your computer/terminal.

DB - 9 PIN CONNECTION	
Pin #	Function
2	Transmit (OUT)
3	Receive (IN)
5	Ground
7	CTS (clear to send) (IN)
8	RTS (request to send) (OUT)
1, 4, 6, 9	Not used

Set your computer/terminal for VT-100 emulation. The serial port on the computer/terminal should be set for: **38.4K baud, 8 data bits, 1 stop bit, no parity and no flow control.**

Main Configuration Screen

After running through an initial self test, the screen will display the following message: “Press <Enter> for Device Configuration.”

Press **Enter** to be taken to the main configuration screen. Here you will find several displays:

Saved Values — *displays changes made during current session.*

- IP Address (MUST be assigned during initial configuration)
- Subnet Mask (MUST be assigned during initial configuration)
- Default Gateway

Current Values — *displays values currently in use.*

- IP Address (IP address of SNMP agent)
- Subnet Mask (mask to define IP subnet agent is connected to)
- Default Gateway (default router for IP traffic outside subnet)

Command List

- **I** = Enter New Saved Parameter Values
- **P** = Change Password
- **T** = New Trap Destination
- **K** = Remove ALL Trap Destinations
- **C** = New Community String
- **U** = Delete ALL Community Strings
- **E** = End Session
- **Space** = Device Specific Configuration

N O T E

You must reboot after making any modifications to the Saved Values or your changes will not take effect. To reboot, type the word “**Reboot**” (no quote marks) at the prompt on the main configuration screen, or turn the chassis power OFF then ON again.

N O T E

Because a Delete key is not available on VT-100 terminal emulators, use the **F2** key instead.

Assigning TCP/IP Information

To modify the Saved Parameter Values (i.e., assign IP address and subnet mask), press **I**. You will be instructed to enter the IP address and subnet mask for the connected device. Press **Enter** after each. You may also assign a default gateway, if desired (press **Enter** to skip).

When finished, press **Enter**, then type “**Reboot**” for changes to take effect. The Saved Values and Current Values should now both display the changes made (e.g., new IP address and subnet mask).

Creating Community Strings

The default community string is named “public” and has read/write access. IMC Networks recommends you set up two communities: one with read-only access (for general use), the other with read/write access (for the administrator). To create a new community string, go to the main configuration screen and press **C**. Enter the name of the new community (up to 16 characters, no spaces) and press **Enter**. Then type one of the following to assign the community string’s access rights:

- **R** = read-only access
- **W** = read/write access
- **Enter** = abort

Press **Enter**.

When finished, press **Enter**, then type “**Reboot**” for changes to take effect. The Saved Values and Current Values should now both display the changes made (e.g., new IP address and subnet mask).

Deleting Community Strings

To delete all community strings and start over, press **U**. You will then be asked, “Are you sure you want to delete all future strings?” Press **Y** to proceed, **N** to abort. Press **Enter**.

Note that the above function will delete ALL community strings. If you want to be able to selectively delete community strings, use *HUBCTRL32* to configure your device.

Assigning Trap Destinations

Traps are sent by the manageable device to a management PC when a certain event takes place.

To enter a trap destination, press **T**. You will then be asked to “Enter a New IP Address.” Type the IP address of the destination device and press **Enter**. Then type the name of the community string (created earlier) and press **Enter**.

Note that the above function enables ALL of the traps the device is capable of. If you want to be able to selectively activate and de-activate traps, use *HUBCTRL32* to configure your device.

Removing Trap Destinations

To remove all trap destinations, press **K**. You will then be asked if you really want to remove all trap destinations. Press **Y** to continue. Press **N** to abort. Press **Enter**.

Password Protection

You can password protect the serial configuration process by pressing **P** from the main configuration screen. You will be asked to enter a password. (**NOTE:** Passwords are case sensitive.) Enter your password (spaces are NOT allowed) and press **Enter**. You will then be asked for your password whenever you log on or off. To remove password protection, select **P** and instead of entering a password, press **Enter**.

Should you forget the password, use *HUBCTRL32* to access the back-up copy of the PROM, then reburn the flash PROM (or contact IMC Networks technical support for assistance).

Ending Your Session

Be sure to press **E** before disconnecting the cable in order to stop the device from outputting to the serial port.

About iView

iView is a cross-platform network management application for IMC Networks intelligent networking devices. It features a graphic user interface (GUI) and gives network managers the ability to monitor and control IMC Networks’ products from virtually any 32-bit Windows platform. *iView* can also function as a snap-in module for many SNMP applications. Visit www.imcnetworks.com/products/iview.htm for more information.

► SYSTEM REQUIREMENTS

To run *iView for FiberLinX TX/FX*, the management PC must be equipped with the following:

- 20 MB free disk space, 32 MB RAM

as well as one of the following operating systems:

- Windows™ 95/98/NT/2000 (standalone or with OpenView)
- HP-UX and OpenView
- IBM AIX and NetView or OpenView
- Solaris and OpenView

NOTE

The HP-UX, IBM AIX, and Solaris versions of *iView* can be downloaded at <http://www.imcnetworks.com/tech/software.htm>.

Please consult the *iView* CD for assistance in installing and launching *iView for FiberLinX TX/FX*.

► USING iVIEW TO MANAGE FIBERLINX TX/FX

iView for FiberLinX TX/FX features a Module Detail Screen, the main viewing screen for *iView for FiberLinX TX/FX*. Depending on whether you are managing a standalone unit or dual (Host/Remote) *FiberLinX TX/FX* units, *iView*’s displays and options will vary.

From within *iView for FiberLinX TX/FX*, you can use its virtual faceplate display(s) to remotely manage your *FiberLinX TX/FX* unit(s). Note that within *iView for FiberLinX TX/FX*, the only end-user configuration options are

creating descriptions for the units and disabling/enabling ports (default on all ports is enabled). The rest of the functions are purely information-related.

For a window-by-window guide to *iView for FiberLinX TX/FX*, please consult the *FiberLinX TX/FX* online help file (choose **Start, Programs, IMC Networks, iView, FiberLinX TX/FX Help**, or use the **Help** menu within *iView for FiberLinX TX/FX*).

➤ **IF USING IVIEW WITH HP OPENVIEW**

During the installation process, *iView* will ask if HP OpenView is installed on the management PC. Click **Yes** to integrate the appropriate files.

You can also manually copy the file **FLINX100.REG** into the appropriate OpenView resource file on the management PC (usually C:\openview\resource\c).

Once in OpenView, highlight the *FiberLinX TX/FX* icon and select the **Tools, FiberLinX TX/FX**; OpenView will then launch *iView*.

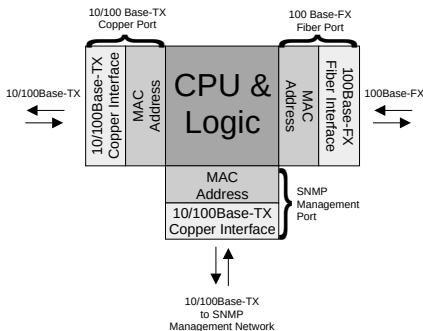
➤ **IF NOT USING IVIEW**

If you will be using another application for management, you will need to integrate the IMC Networks SNMP vendor files (a.k.a. MIBs) into your application. Consult the documentation of your SNMP-manageable NMS for details. **FLINX.MIB** must be integrated into the management software to successfully manage *FiberLinX TX/FX*.

How FiberLinX TX/FX Works

The movement of data from one port to another is accomplished via packet forwarding. The destination address of each Ethernet packet entering the *FiberLinX TX/FX* is checked to determine whether it is a management packet or a downstream data packet, and is forwarded appropriately. Packets not addressed for management ports are sent through to the network. Similarly, management packets are forwarded internally to the management engine and are not forwarded.

More information about how *FiberLinX TX/FX* works can be found on the IMC Networks Web site at www.imcnetworks.com.



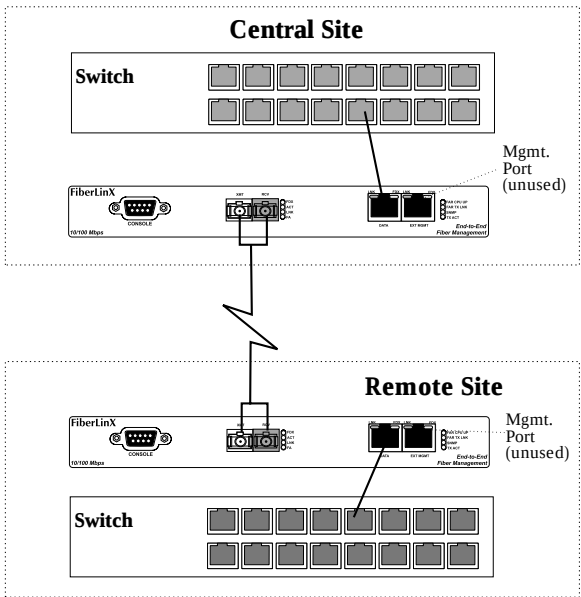
Application Examples

FiberLinX TX/FX can be used in many configurations based upon application, network architecture and management security requirements. The following pages show three examples of how you can use *FiberLinX TX/FX* in your network.

Example 1

FIBER CONVERSION AND REMOTE MANAGEMENT BETWEEN TWO COPPER-BASED SWITCHES

In this situation, configure the Central site's unit as a Host with management traffic through the twisted pair data port, and the Remote site's unit to accept management traffic through the fiber data port.



Note that the twisted pair management ports on both *FiberLinX TX/FX* remain unused.

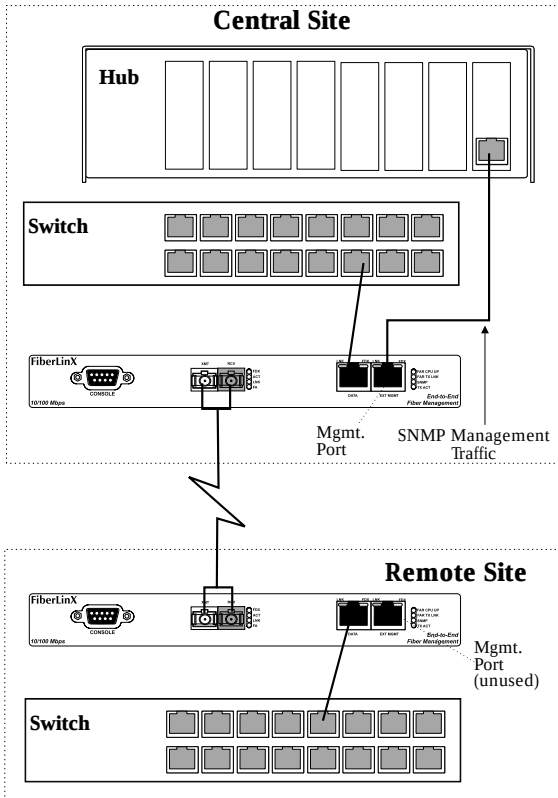
Configure the two *FiberLinX TX/FX* units used in this example exactly as the ones in Example 2, except direct management traffic on the Central site's unit to the twisted pair management port.

Example 1: DIP Switch Settings					
	Switch 7 (S1)	Switch 8 (S1)	Switch 1 (S3)	Switch 2 (S3)	Switch 3 (S3)
Central (Host)	OFF	ON	OFF	ON	OFF
Remote	ON	OFF	OFF	OFF	OFF

Example 2

FIBER CONVERSION AND HIGHLY SECURE REMOTE MANAGEMENT BETWEEN TWO COPPER-BASED SWITCHES

For the highest level of management security, route SNMP management traffic completely away from the switch. Two *FiberLinX TX/FX* units are also used in this configuration. The following illustration shows an external hub being used to maintain LAN separation.



NOTE

You can access and manage the Remote site's *FiberLinX TX/FX* directly in this configuration if you assign the unit an IP address.

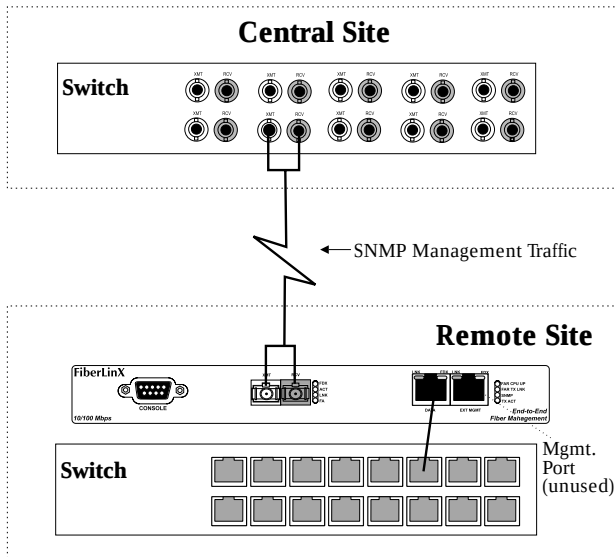
Example 2: DIP Switch Settings

	Switch 7 (S1)	Switch 8 (S1)	Switch 1 (S3)	Switch 2 (S3)	Switch 3 (S3)
Central (Host)	OFF	ON	ON	OFF	OFF
Remote	ON	OFF	OFF	OFF	OFF

Example 3

DIRECT FIBER SWITCH CONNECTION FROM CENTRAL TO REMOTE SITE

To achieve remote management and monitoring capabilities, directly connect a *FiberLinX TX/FX* to a fiber-based switch. All SNMP management traffic and data traffic goes straight into the switch at the Central site via the fiber port. SNMP management traffic is imbedded within the corporate network, but no management data passes to the Remote site.



Configure *FiberLinX TX/FX* to accept SNMP management traffic from the fiber port. In this application, *FiberLinX TX/FX* is neither a Host nor Remote unit. The twisted pair management port on this *FiberLinX TX/FX* is unused.

Example 3: DIP Switch Settings

Switch 7 (S1)	Switch 8 (S1)	Switch 1 (S3)	Switch 2 (S3)	Switch 3 (S3)
OFF	OFF	OFF	OFF	ON

Troubleshooting

- If *FiberLinX TX/FX* is connected to a non-negotiating device, sometimes the Duplex mode will not auto-negotiate. This can be fixed by changing the settings in *iView*.

- 4) After removal, always place the boards on a grounded, static free surface, ESD pad or in a proper ESD bag. Do not slide the board over any surface.

WARRANTY

IMC Networks warrants to the original end-user purchaser that this product, EXCLUSIVE OF SOFTWARE, shall be free from defects in materials and workmanship under normal and proper use in accordance with IMC Networks' instructions and directions for a period of six (6) years after the original date of purchase. This warranty is subject to the limitations set forth below.

At its option, IMC Networks will repair or replace at no charge the product which proves to be defective within such warranty period. This limited warranty shall not apply if the IMC Networks product has been damaged by unreasonable use, accident, negligence, service or modification by anyone other than an authorized IMC Networks Service Technician or by any other causes unrelated to defective materials or workmanship. Any replaced or repaired products or parts carry a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

To receive in-warranty service, the defective product must be received at IMC Networks no later than the end of the warranty period. The product must be accompanied by proof of purchase, satisfactory to IMC Networks, denoting product serial number and purchase date, a written description of the defect and a Return Merchandise Authorization (RMA) number issued by IMC Networks. No products will be accepted by IMC Networks which do not have an RMA number. For an RMA number, contact IMC Networks at PHONE: (800) 624-1070 (in the U.S and Canada) or (949) 465-3000 or FAX: (949) 465-3020. The end-user shall return the defective product to IMC Networks, freight, customs and handling charges prepaid. End-user agrees to accept all liability for loss of or damages to the returned product during shipment. IMC Networks shall repair or replace the returned product, at its option, and return the repaired or new product to the end-user, freight prepaid, via method to be determined by IMC Networks.

IMC Networks shall not be liable for any costs of procurement of substitute goods, loss of profits, or any incidental, consequential, and/or special damages of any kind resulting from a breach of any applicable express or implied warranty, breach of any obligation arising from breach of warranty, or otherwise with respect to the manufacture and sale of any IMC Networks product, whether or not IMC Networks has been advised of the possibility of such loss or damage.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, IMC NETWORKS MAKES NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS IMC NETWORKS PRODUCT, INCLUDING WITHOUT LIMITATION ANY SOFTWARE ASSOCIATED OR INCLUDED. IMC NETWORKS SHALL DISREGARD AND NOT BE BOUND BY ANY REPRESENTATIONS OR WARRANTIES MADE BY ANY OTHER PERSON, INCLUDING EMPLOYEES, DISTRIBUTORS, RESELLERS OR DEALERS OF IMC NETWORKS, WHICH ARE INCONSISTENT WITH THE WARRANTY SET FORTH ABOVE. ALL IMPLIED WARRANTIES INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY LIMITED TO THE DURATION OF THE EXPRESS WARRANTY STATED ABOVE.

Every reasonable effort has been made to ensure that IMC Networks product manuals and promotional materials accurately describe IMC Networks product specifications and capabilities at the time of publication. However, because of ongoing improvements and updating of IMC Networks products, IMC Networks cannot guarantee the accuracy of printed materials after the date of publication and disclaims liability for changes, errors or omissions.

FEDERAL COMMUNICATIONS COMMISSION RADIO FREQUENCY INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class A computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Questions or Comments about this manual? Contact techdocs@imcnetworks.com.



19772 Pauling • Foothill Ranch, CA 92610-2611 USA

TEL: (949) 465-3000 • FAX: (949) 465-3020

www.imcnetworks.com

© 2001 IMC Networks. All rights reserved.

The information in this document is subject to change without notice. IMC Networks assumes no responsibility for any errors that may appear in this document. **FiberLinX TX/FX** is a trademark of IMC Networks. Other brands or product names may be trademarks and are the property of their respective companies.

Document Number 50-80211-00 A1

August 2001